

599R/2774500

#4

USPTO
09/442727
JC568 U.S. PTO
Barcode

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1998年11月19日

願番号
Application Number:

平成10年特許願第329973号

願人
Applicant(s):

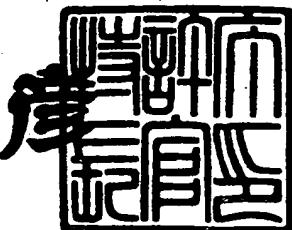
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 9月24日

特許庁長官
Commissioner,
Patent Office

近藤 隆



【書類名】 特許願
【整理番号】 9800713305
【提出日】 平成10年11月19日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 29/00
【発明の名称】 信号処理回路
【請求項の数】 8
【発明者】
【住所又は居所】 神奈川県横浜市保土ヶ谷区神戸町134番地 ソニー・エルエスアイ・デザイン株式会社内
【氏名】 佐藤 貞治
【特許出願人】
【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代表者】 出井 伸之
【代理人】
【識別番号】 100094053
【弁理士】
【氏名又は名称】 佐藤 隆久
【手数料の表示】
【予納台帳番号】 014890
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9707389
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 信号処理回路

【特許請求の範囲】

【請求項1】 送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインターフェースバスに送出する信号処理回路であつて、

送信すべきデータを所定の暗号モードで暗号化し、暗号化情報とともに出力する暗号処理回路と、

暗号処理回路で暗号化されたデータに、その暗号化情報を付加して上記シリアルインターフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連續性を確認し、不連續性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインターフェースバスに送信する送信回路とを有する信号処理回路。

【請求項2】 上記送信回路は、上記暗号化情報をパケットのヘッダの所定の領域に設定する

請求項1記載の信号処理回路。

【請求項3】 送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインターフェースバスに送出する信号処理回路であつて、

少なくとも一つの暗号モード情報が設定される保持手段と、

送信データを暗号化すべきモードを指定する制御手段と、

上記制御手段で指定された暗号モード情報を選択する暗号モード選択回路と、上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報をともに出力する暗号エンジン回路とを有する暗号処理回路と、

暗号処理回路で暗号化されたデータに、その暗号化情報を付加して上記シリアルインターフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回

路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインターフェースバスに送信する送信回路とを有する信号処理回路。

【請求項4】 上記送信回路は、上記暗号化情報をパケットのヘッダの所定の領域に設定する

請求項3記載の信号処理回路。

【請求項5】 送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインターフェースバスに送出する信号処理回路であつて、

記憶手段と、

少なくとも一つの暗号モード情報が設定される保持手段と、
送信データを暗号化すべきモードを指定する制御手段と、
上記制御手段で指定された暗号モード情報を選択する暗号モード選択回路と、
上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともにに出力する暗号エンジン回路とを有する暗号処理回路と、

受信側で受信データをアプリケーション側へ出力すべき時間情報を生成し、当該時間情報に上記暗号処理回路による暗号化情報を付加して上記暗号化データとともに上記記憶手段に格納する第1の送信回路と、

上記記憶手段に格納された時間情報および暗号化情報が付加された暗号化データを読み出し、所定フォーマットのパケットデータを生成するとともに、そのパケットヘッダに上記暗号化情報を設定して上記シリアルインターフェースバスに送信し、かつ、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインターフェースバスに送信する第2の送信回路と

を有する信号処理回路。

【請求項6】 送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインターフェースバスに送出し、あらかじめ決められた時間サイクルでシリアルインターフェースバスを送信される、データが暗号化され、少なくともその暗号化情報を含むパケットデータを受信してアプリケーション側に出力する信号処理回路であって、

送信時には、送信すべきデータを所定の暗号モードで暗号化し、受信時には受信パケットデータに含まれる暗号化情報を基づいて受信した暗号化データを復号してアプリケーション側へ出力する暗号処理回路と、

暗号処理回路で暗号化されたデータに、その暗号化情報を付加して上記シリアルインターフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報をから暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインターフェースバスに送信する送信回路とを有する信号処理回路。

【請求項7】 上記送信回路は、上記暗号化情報をパケットのヘッダの所定の領域に設定する

請求項6記載の信号処理回路。

【請求項8】 送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインターフェースバスに送出し、あらかじめ決められた時間サイクルでシリアルインターフェースバスを送信される、データが暗号化され、少なくともその暗号化情報を含むパケットデータを受信してアプリケーション側に出力する信号処理回路であって、

第1の記憶手段と、

第2の記憶手段と、

少なくとも一つの暗号モード情報が設定される保持手段と、

送信データを暗号化すべきモードを指定する制御手段と、

受信パケットデータから上記時間情報および暗号化データに上記暗号化情報を

付加して上記記憶手段に格納する第1の受信回路と、

上記記憶手段に格納された暗号化情報および暗号化データを出力するとともに、時間情報に基づいて受信データをアプリケーション側へ出力すべき時間を指示する第2の受信回路と、

上記第2の受信回路による暗号化情報から暗号化データが暗号化された暗号モードを検出する暗号モード検出回路と、上記制御手段で指定された暗号モード情報または上記暗号モード検出回路で検出した暗号モード情報を上記保持手段に設定された情報の中から選択する暗号モード選択回路と、送信時には上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともに出力し、受信時には上記暗号モード選択回路で選択された暗号モードで上記受信データを復号して、復号データを上記第2の受信回路により指示された時間にアプリケーション側へ出力する暗号エンジン回路とを有する暗号処理回路と、

受信側で受信データをアプリケーション側へ出力すべき時間情報を生成し、当該時間情報に上記暗号処理回路による暗号化情報を付加して上記暗号化データとともに上記記憶手段に格納する第1の送信回路と、

上記記憶手段に格納された時間情報および暗号化情報が付加された暗号化データを読み出し、所定フォーマットのパケットデータを生成するとともに、そのパケットヘッダに上記暗号化情報を設定して上記シリアルインターフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連續性を確認し、不連續性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインターフェースバスに送信する第2の送信回路と

を有する信号処理回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタルシリアルインターフェースに用いられる信号処理回路に係

り、特にデータの暗号化回路に関するものである。

【0002】

【従来の技術】

近年、マルチメディア・データ転送のためのインターフェースとして、高速データ転送、リアルタイム転送を実現する IEEE (The Institute of Electrical and Electronic Engineers) 1394、High Performance Serial Bus が規格化された。

【0003】

この IEEE 1394 シリアルインターフェースのデータ転送には、従来の Request, Acknowledge の要求、受信確認を行うアシンクロナス (Asynchronous) 転送と、あるノードから $125 \mu s$ に 1 回必ずデータが送られるアイソクロナス (Isochronous) 転送がある。

【0004】

このように、2つの転送モードを有する IEEE 1394 シリアルインターフェースでのデータは、パケット単位で転送が行われる。

【0005】

図10は、アイソクロナス通信における1ソースパケットのバイトサイズを示す図である。図10 (A) はDVB (Digital Video Broadcast) 仕様時、図10 (B) はDSS (Digital Satellite System) 仕様時のパケットサイズを示している。

【0006】

DVB仕様時のソースパケットサイズは、図10 (A) に示すように、4バイトのソースパケットヘッダ (SPH; Source Packet Header) と188バイトのトランスポートストリームデータの192バイトである。

【0007】

これに対して、DSS仕様時のソースパケットサイズは、図10 (B) に示すように、4バイトのソースパケットヘッダ (SPH)、10バイトの付加データ、および130バイトのデータの144バイトである。

付加バイトはソースパケットヘッダとデータとの間に挿入される。なお、IE

IEEE1394規格では、取り扱う最小データの単位は1クワドレット(quadlet)(=4バイト=32ビット)であるため、トランSPORTストリームデータと付加データの合計が32ビット単位で構成できる設定が必要である。

ただし、デフォルトでは付加バイトなしで設定される。

【0008】

図11は、IEEE1394規格のアイソクロナス通信でデータを送信させるときの元のデータと、実際に送信されるパケットとの対応関係の一例を示す図である。

【0009】

図11に示すように、元のデータであるソースパケットは、4バイトのソースパケットヘッダと、データ長を調整するためのパディングデータを付加された後、所定の数のデータブロックに分割される。

なお、パケットを転送するときのデータの単位が1クワドレット(4バイト)であることから、データブロックや各種ヘッダなどのバイト長は、全て4の倍数に設定される。

【0010】

図12は、ソースパケットヘッダのフォーマットを示す図である。

図12に示すように、ソースパケットヘッダのうち、25ビットには、たとえば上述したDVB方式等のデジタル衛星放送等で利用されているMPEG(Moving Picture Experts Group)-TS(Transport Stream)データをアイソクロナス通信で送信するときに、ジッタを抑制するために利用されるタイムスタンプ(Time Stamp)が書き込まれる。

【0011】

そして、このようなパケットヘッダやCIP(Common Isochronous Packet)ヘッダ等のデータが、所定の数のデータブロックに付加されることによりパケットが生成される。

【0012】

図13はアイソクロナス通信用パケットの基本構成例を示す図である。

図13に示すように、アイソクロナス通信のパケットは、第1クワドレットが

1394ヘッダ(Header)、第2クワドレットがヘッダCRC(Header-CRC)、第3クワドレットがCIPヘッダ1(CIP-Header1)、第4クワドレットがCIPヘッダ2(CIP-Header2)、第5クワドレットがソースパケットヘッダ(SPH)で、第6クワドレット以降がデータ領域である。そして、最後のクワドレットがデータCRC(Data-CRC)である。

【0013】

1394ヘッダは、データ長を表すdata-length、このパケット転送されるチャネルの番号(0~63のいずれか)を示すchannel、処理のコードを表すtcod e、および各アプリケーションで規定される同期コードsyにより構成されている。

ヘッダCRCは、パケットヘッダの誤り検出符号である。

【0014】

CIPヘッダ1は、送信ノード番号のためのSID(Source node ID)領域、データブロックの長さのためのDBS(Data Block Size)領域、パケット化におけるデータの分割数のためのFN(Fraction Number)領域、パディングデータのクワドレット数のためのQPC(Quadlet Padding Count)領域、ソースパケットヘッダの有無を表すフラグのためのSPH領域、アイソクロナスパケットの数を検出するカウンタのためのDBC(Data Block Continuity Counter)領域により構成されている。

なお、DBS領域は、1アイソクロナスパケットで転送するクワドレット数を表す。

【0015】

CIPヘッダ2は、転送されるデータの種類を表す信号フォーマットのためのFMT領域、および信号フォーマットに対応して利用されるFFD(Format Dependent Field)領域により構成されている。

【0016】

SPHヘッダは、トランSPORTストリームパケットが到着した時間に固定の遅延値を加えた値が設定されるタイムスタンプ領域を有している。

また、データCRCは、データフィールドの誤り検出符号である。

【0017】

上述した構成を有するパケットの送受信を行うIEEE1394シリアルインターフェースの信号処理回路は、図14に示すように、主としてIEEE1394シリアルバスを直接ドライブするフィジカル・レイヤ回路1と、フィジカル・レイヤ回路1のデータ転送をコントロールするリンク・レイヤ回路2とにより構成される。

【0018】

上述したIEEE1394シリアルインターフェースにおけるアイソクロナス通信系では、たとえば図14に示すように、リンク・レイヤ回路2はフィジカル・レイヤ回路1を介してシリアルインターフェースバスBSに接続されている。

そして、リンク・レイヤ回路2には、MPEGトランスポータやDVC(R(Digital Video Cassette Recorder)等のアプリケーション側回路3が接続される。

【0019】

【発明が解決しようとする課題】

ところで、現在、映画やテレビ放送などの映像データは、著作権との関係等から不正コピーを防止するため、家庭等では、自由にデジタル記録できない。したがって、たとえばデジタル衛星放送用のセット・トップ・ボックスにはデジタルの出力端子が設けられていない。

【0020】

しがしながら、IEEE1394シリアルインターフェースは、映像や音楽などのデジタルデータを異なる機器間で送受信するインターフェースであり、また、近年、家庭用のデジタル録画機器の開発が盛んに行われ、実用に供されてくるようになってきた現状では、家庭等でデジタル記録を行う機会が増えてくることは避けられないことである。

したがって、このような状況に鑑みて不正コピーを有効に防止する機能が必要であるが、IEEE1394シリアルインターフェースの信号処理回路では、その機能を備えた構成は未だ実現されていない。

【0021】

また、この暗号化機能を実現した場合には、連続して複数のパケットデータを

送信する場合に、一つの転送サイクル内で、異なる暗号モードで暗号化されたデータが混在していると、受信側で暗号モードを判別できず、復号できないという不都合が生じないように構成する必要がある。

【0022】

本発明は、かかる事情に鑑みてなされたものであり、その目的は、異なる機器間で送信または受信するディジタルデータの不正なコピーを防止できる、かつ複数の暗号モードを判別できず、復号できなくなることを防止でき、受信側において受信データを正しく復号することができる信号処理回路を提供することにある。

【0023】

【課題を解決するための手段】

上記目的を達成するため、本発明は、送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出する信号処理回路であって、送信すべきデータを所定の暗号モードで暗号化し、暗号化情報とともに出力する暗号処理回路と、暗号処理回路で暗号化されたデータに、その暗号化情報を附加して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する送信回路とを有する。

【0024】

また、本発明では、上記送信回路は、上記暗号化情報をパケットのヘッダの所定の領域に設定する。

【0025】

また、本発明は、送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出する信号処理回路であって、少なくとも一つの暗号モード情報が設定される保持手段と、送信データを暗号化すべきモードを指定する制御手段と、上記制御手段で指定された暗号モード

情報を選択する暗号モード選択回路と、上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともにに出力する暗号エンジン回路とを有する暗号処理回路と、暗号処理回路で暗号化されたデータに、その暗号化情報を附加して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連續性を確認し、不連續性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する送信回路とを有する。

【0026】

また、本発明は、送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出する信号処理回路であつて、記憶手段と、少なくとも一つの暗号モード情報が設定される保持手段と、送信データを暗号化すべきモードを指定する制御手段と、上記制御手段で指定された暗号モード情報を選択する暗号モード選択回路と、上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともにに出力する暗号エンジン回路とを有する暗号処理回路と、受信側で受信データをアプリケーション側へ出力すべき時間情報を生成し、当該時間情報に上記暗号処理回路による暗号化情報を附加して上記暗号化データとともに上記記憶手段に格納する第1の送信回路と、上記記憶手段に格納された時間情報および暗号化情報が付加された暗号化データを読み出し、所定フォーマットのパケットデータを生成するとともに、そのパケットヘッダに上記暗号化情報を設定して上記シリアルインタフェースバスに送信し、かつ、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連續性を確認し、不連續性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する第2の送信回路とを有する。

【0027】

また、本発明は、送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出し、あらかじめ決められた時間サイクルでシリアルインタフェースバスを送信される、データが暗号化され、少なくともその暗号化情報を含むパケットデータを受信してアプリケーション側に出力する信号処理回路であって、送信時には、送信すべきデータを所定の暗号モードで暗号化し、受信時には受信パケットデータに含まれる暗号化情報に基づいて受信した暗号化データを復号してアプリケーション側へ出力する暗号処理回路と、暗号処理回路で暗号化されたデータに、その暗号化情報を附加して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する送信回路とを有する。

[0028]

ード情報を上記保持手段に設定された情報の中から選択する暗号モード選択回路と、送信時には上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともにに出力し、受信時には上記暗号モード選択回路で選択された暗号モードで上記受信データを復号して、復号データを上記第2の受信回路により指示された時間にアプリケーション側へ出力する暗号エンジン回路とを有する暗号処理回路と、受信側で受信データをアプリケーション側へ出力すべき時間情報を生成し、当該時間情報に上記暗号処理回路による暗号化情報を付加して上記暗号化データとともに上記記憶手段に格納する第1の送信回路と、上記記憶手段に格納された時間情報および暗号化情報が付加された暗号化データを読み出し、所定フォーマットのパケットデータを生成するとともに、そのパケットヘッダに上記暗号化情報を設定して上記シリアルインターフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインターフェースバスに送信する第2の送信回路とを有する。

【0029】

本発明によれば、送信すべきデータは、暗号化処理回路において指定された暗号モードで暗号化される。

そして、暗号化されたデータは、その暗号化の情報とともに、たとえば記憶手段に一旦格納される。

そして、送信回路により記憶手段から読み出され、たとえば格納された暗号化情報が所定フォーマットのパケットのヘッダに設定されて、暗号化データとともに、あらかじめ決められた時間サイクルでシリアルインターフェースバスに送出される。

また、データ送信において、複数のパケットの送信時には、送信回路で、暗号処理回路による暗号化情報から暗号モードの連続性が確認される。

その結果、不連続性が確認されたときは、あらかじめ決められた時間サイクル

で送信できる帯域に余裕があったとしても送信が停止され、異なる暗号モードで暗号化されたデータは、次のサイクルでパケットデータとして上記シリアルインターフェースバスに送信される。

【0030】

また、本発明によれば、シリアルインターフェースバスを転送されたパケットデータは受信回路に入力される。

受信回路では、受信パケットデータから暗号化情報および暗号化データが抽出され、たとえば記憶手段に格納される。

記憶手段に格納された暗号化情報および暗号化データは、暗号処理回路に読み出される。

そして、暗号処理回路においては、読み出した暗号化情報に基づいて受信暗号化データが復号されてアプリケーション側へ出力される。

【0031】

【発明の実施の形態】

図1は、IEEE1394シリアルインターフェースに適用される本発明に係る信号処理回路の一実施形態を示すブロック構成図である。

【0032】

この信号処理回路は、リンク・レイヤ回路10、フィジカル・レイヤ回路20、ホストコンピュータとしてのCPU30により構成されている。また、リンクレイヤ回路10には、アプリケーション側回路40が接続されている。

アプリケーション側回路40は、図1に示すように、MPEGトランスポータ41、D/A(Digital/Analog)コンバータ42、IEC958デジタルオーディオ回路43により構成される。また、44はクロック供給回路としてのPLL回路を示している。

なお、以下では、アプリケーション側回路4をMPEGトランスポータ41として説明する。

【0033】

リンク・レイヤ回路10は、CPU30の制御の下、シンクロナス転送およびアイソクロナス転送の制御、並びにフィジカル・レイヤ回路20の制御を行う

具体的には、図1に示すように、リンクコア(Link Core)101、ホストインターフェース回路(HOST I/F)102、アプリケーションインターフェース回路(AP I/F)103、アシンクロナス通信の送信用FIFO(AT-FIFO)104、アシンクロナス通信の受信用FIFO(AR-FIFO)105、インサートパケットバッファ(IPB)106、暗号処理回路(CPH)107、第1の送信回路としてのアイソクロナス通信用送信前処理回路(TXOPRE)108、第2の送信回路としてのアイソクロナス通信用送信後処理回路(TXOPRO)109、第1の受信回路としてのアイソクロナス通信用受信前処理回路(TXIPRE)110、第2の受信回路としてのアイソクロナス通信用受信後処理回路(TXIPRO)111、アイソクロナス通信の送信用FIFO(IT-FIFO)112、アイソクロナス通信の受信用FIFO(IR-FIFO)113および保持手段としてのコンフィギュレーションレジスタ(Configuration Register、以下CFRという)114により構成されている。

【0034】

図1の回路において、ホストインターフェース回路102、送信用FIFO104、受信用FIFO105およびリンクコア101によりアシンクロナス通信系回路が構成される。

そして、アプリケーションインターフェース回路103、暗号処理回路107、送信前処理回路108、送信後処理回路109、受信前処理回路110、受信後処理回路111、送信用FIFO112、受信用FIFO113およびリンクコア101によりアイソクロナス通信系回路が構成される。

【0035】

リンクコア101は、アシンクロナス通信用パケットおよびアイソクロナス通信用パケットの送信回路、受信回路、これらパケットのIEEE1394シリアルバスBSを直接ドライブするフィジカル・レイヤ回路20とのインターフェース回路、125μs毎にリセットされるサイクルタイマ、サイクルモニタやCRC回路から構成されている。そして、たとえばサイクルタイマ等の時間データ等はCFR111を通してアイソクロナス通信系処理回路に供給される。

【0036】

ホストインターフェース回路102は、主としてホストコンピュータとしてのCPU30と送信用 FIFO104、受信用 FIFO105とのシンクロナス通信用パケットの書き込み、読み出し等の調停、並びに、CPU30とCFR114との各種データの送受信の調停を行う。

たとえばCPU30からは、アイソクロナスパケットを暗号化する、後述する複数のモード（キー；key）が設定され、設定された暗号モードのうちの一つを選択して暗号処理回路107が暗号化すべき暗号キー選択情報が、ホストインターフェース102を通してCFR114にセットされる。

また、たとえばCPU30からは、アイソクロナス通信用パケットのSPH（ソースパケットヘッダ）に設定されるタイムスタンプ用遅延時間Txdelayがホストインターフェース102を通してCFR114にセットされる。

さらに、CPU30からは、たとえば通常のMPEGのトランスポートストリームデータの間に制御用パケットであるインサートパケットデータを挿入する必要が生じたとき、CFR114のレジスタIPTxGoに論理「1」がセットされる。

【0037】

アプリケーションインターフェース回路103は、アプリケーション側回路40、たとえばMPEGトランスポータ41と暗号処理回路107と制御信号等を含む、暗号化前および復号化後のデータの送受信の調停を行う。

【0038】

送信用 FIFO104には、IEEE1394シリアルバスBSに伝送させるシンクロナス通信用パケットが格納され、受信用 FIFO105にはIEEE1394シリアルインターフェースバスBSを伝送されてきたシンクロナス通信用パケットが格納される。

【0039】

インサートパケットバッファ106には、たとえば所望のパケットデータがCPU30から書き込まれる。

インサートパケットバッファ106の容量は、たとえば188バイトであり、

188バイトまでのデータが有効で、この容量を超えたデータに関しては送信されない。

送信するデータが188バイト以下の場合には、書き込まれたデータ以外が「1」にセットされて送信される。

インサートパケットバッファ106に一度書き込まれたデータは、再び書き込みが行われるまで、その値を保持される。

インサートパケットバッファ106に書き込まれたデータは、暗号処理回路107で暗号化されて送信前処理回路108を介して送信用FIFO112に転送されるが、転送時には、上述したCFR114のレジスタIPTxGoが「1」に設定され、転送が終了した場合には自動的に「0」に設定され、CPU30はこれを確認することで転送終了を確認する。

【0040】

暗号処理回路107は、データ送信時には、CPU30からCFR114に設定された暗号キー選択情報に基づき、CPU30からCFR114に設定された複数の暗号モード（キー；key）のうち一の暗号キーを選択し、選択しが暗号キーにより、アプリケーションインターフェース回路103を介して入力した送信すべきデータをたとえば所定の共通鍵暗号方式により暗号化し、送信前処理回路108に出力する。

また、暗号処理回路107は、受信後処理回路111を介して入力した暗号化されたデータの暗号化に用いられた暗号モード（キー）を検出し、その暗号キー情報に基づいて暗号化データを復号してアプリケーションインターフェース回路103に出力する。

【0041】

ここで、暗号モードおよび暗号キーの例について図2に関連付けて説明する。

暗号モードには、図2（A）に示すように、モードA、モードB、およびモードCの3種類があり、これに加えて暗号化なしもある。

そし、各暗号モードA、B、Cの内容は次の通りである。

暗号モードAはコピーを認めない(Never Copy)、暗号モードBは一度だけコピーを認める(Copy Once)、暗号モードCはこれ以上のコピーを認めないおよび暗

号化しない(No More Copy)である。

また、暗号キーには、図2 (B) に示すように、偶数(Even)キー、および奇数(odd)キーの2種類がある。

したがって、暗号化を行う暗号キーとしては、①モードA, 奇数、②モードA, 偶数、③モードB, 奇数、④モードB, 偶数、⑤モードC, 奇数、⑥モードC, 偶数の6種類がある。

【0042】

図3は、暗号処理回路107の構成例を示すブロック図である。

暗号処理回路107は、図3に示すように、暗号モード選択回路1071、暗号モード検出回路1072、マルチプレクサ1073、および暗号エンジン回路1074により構成されている。

【0043】

暗号モード選択回路1071は、データ送信時には、CPU30からCFR114に設定された暗号キー選択信号(情報)S114に基づき、CPU30からCFR114に設定された6個の暗号モード(キー；key)のうちの一の暗号キーを選択し、暗号エンジン回路1074に出力する。

また、データ受信時には、暗号モード検出回路1072からの暗号キー選択信号S1072に基づき、CPU30からCFR114に設定された6個の暗号モード(キー；key)のうち、一の暗号キーを選択し、暗号エンジン回路1074に出力する。

【0044】

暗号モード検出回路1072は、受信後処理回路111を介して入力し暗号化情報から、データの暗号化に用いられた暗号モード(キー)を検出し、検出結果を暗号キー選択信号S1072として暗号モード選択回路1071に出力する。

【0045】

マルチプレクサ1073は、送信時にはアプリケーションインターフェース回路103を介した送信データを暗号エンジン回路1074に入力させ、受信時には受信後処理回路111による暗号化されている受信データを暗号エンジン回路1074に入力させる。

【0046】

暗号エンジン回路1074は、送信時には、マルチプレクサ1073を介して入力した送信データを、暗号モード選択回路1071により指定された暗号キーに基づいて暗号化してその暗号化情報とともに送信前処理回路108に出力し、受信時には、マルチプレクサ1073を介して入力した受信データを、暗号モード選択回路1071により指定された暗号キーに基づいて暗号化データを復号してアプリケーションインターフェース回路103に出力する。

【0047】

送信前処理回路108は、暗号処理回路107による送信しえべき暗号化データを受けて、IEEE1394規格のアイソクロナス通信用としてクワドレット（4バイト）単位にデータ長を調整し、かつ4バイト（+4ビット）のソースパケットヘッダ（S P H）を付加し、送信用FIFO112に格納する。

【0048】

送信前処理回路108は、送信用FIFO112に送信データを格納するに際して、図4（A）に示すように、4バイト（0～31ビット）のソースパケットヘッダに4ビット（32～36ビット）を付加し、この付加ビットのうちの33ビット、34ビット、および35ビットの3ビットを用いて暗号化情報を設定して格納するとともに、図4（B）に示すように、データ領域の4バイト（0～31ビット）の最大長を示すデータペイロード（Data Payload）に同じく4ビット（32～36ビット）を付加し、この付加ビットのうちの33ビット、34ビット、および35ビットの3ビットを用いて暗号化情報を設定して格納する。

【0049】

暗号化情報は、モードがビット〔35：34〕の2ビットで示され、キーの種類をビット〔33〕の1ビットで示され、内容に応じてこれら3ビットが、図2中s y〔3：2〕およびs y〔1〕のように設定される。ただし、ビット32は未使用である。

すなわち、モードAで偶数キーの場合には〔111〕、モードBで偶数キーの場合には〔101〕、モードCで偶数キーの場合には〔011〕、モードAで奇数キーの場合には〔110〕、モードBで奇数キーの場合には〔100〕、モー

ドCで奇数キーの場合には〔010〕に設定される。

また、暗号化なしの場合には、ビット〔35:34〕が〔00〕に設定される。このとき、ビット〔33〕は意味を持たない。

【0050】

また、送信前処理回路108は、ソースパケットヘッダを付加するときに受信側のデータ出力時間を決定するタイムスタンプを設定するが、この設定は以下のように行われる。

まず、アプリケーション側回路40、たとえばMPEGトランスポータ41からパケットの最終データを受け取ったタイミングで内部のサイクルレジスタの値をラッチする。

次に、CPU30からホストインターフェース102を介してCFR114にセットされた遅延時間Txdelayを上記サイクルレジスタの値に加算する。

そして、加算した値をタイムスタンプとして、受け取ったパケットのソースパケットヘッダに挿入（設定）する。

【0051】

図4（A）は、ソースパケットヘッダにおけるタイムスタンプの具体的な構成を説明するための図である。

図4（A）に示すように、受信側のデータ出力時間を決定するためのタイムスタンプは、25ビットで現時刻を表す。

すなわち、タイムスタンプは25ビットで構成され、下位12ビットがサイクルオフセットCO（cycle-offset）領域、上位13ビットがサイクルカウントCC（cycle-count）領域として割り当てられている。

サイクルオフセットは0～3071（12b 101111111111）の125μsをカウントし（クロックCLK=24.576MHz）、サイクルカウントは0～7999（13b 111110011111）の1秒をカウントするものである。

したがって、原則として、タイムスタンプの下位12ビットは3072以上を示すことはなく、上位13ビットは8000以上を示すことはない。

【0052】

送信後処理回路109は、送信用FIFO112に格納されたソースパケットヘッダを含むデータに対して図5および図13に示すように、1394ヘッダ、CIPヘッダ1、2を付加してリンクコア101の送信回路に出力する。

具体的には、図5に示すように、データ長を表すdata-length、このパケット転送されるチャネルの番号（0～63のいずれか）を示すchannel、処理のコードを表すtcode、および暗号化情報を示すs_yにより構成した1394ヘッダ、さらに図13に示すように、送信ノード番号のためのS I D (Source node ID)領域、データブロックの長さのためのD B S (Data Block Size)領域、パケット化におけるデータの分割数のためのF N (Fraction Number)領域、パディングデータのクワドレット数のためのQ P C (Quadlet Padding Count)領域、ソースパケットヘッダの有無を表すフラグのためのS P H領域、アイソクロナスパケットの数を検出するカウンタのためのD B C領域により構成したCIPヘッダ1、並びに転送されるデータの種類を表す信号フォーマットのためのF M T領域、および信号フォーマットに対応して利用されるF D F (Format Dependent Field)領域により構成したCIPヘッダ2を付加する。

【0053】

なお、1394ヘッダに設定される暗号化情報s_yは、1394ヘッダのビット[3, 2, 1]の3ビットが割り当てられる。その内容は、FIFO112に格納されたソースパケットヘッダに付加された暗号化情報に基づいて設定される。

暗号化情報は、モードがビット[3:2]の2ビットで示され、キーの種類をビット[1]の1ビットで示され、内容に応じてこれら3ビットが、図2中s_y[3:2]およびs_y[1]のように設定される。

すなわち、モードAで偶数キーの場合には[111]、モードBで偶数キーの場合には[101]、モードCで偶数キーの場合には[011]、モードAで奇数キーの場合には[110]、モードBで奇数キーの場合には[100]、モードCで奇数キーの場合には[010]に設定される。

また、暗号化なしの場合には、ビット[3:2]が[00]に設定される。こ

のとき、ビット〔1〕は意味を持たない。

【0054】

また、送信後処理回路109は、図6に示すように、複数のパケットの送信時に、FIFO112から送信データを読み出した際に暗号モードの連續性を確認し、不連續性を確認したときは、その1394規格の送信サイクルで送信できる帯域に余裕があったとしても送信を停止させ、次のサイクルで異なる暗号キーで暗号化されたパケットを送信するように、リンクコア101の送信回路に指示する暗号モード連續性判定回路1091を有している。

【0055】

暗号モード連續性判定回路1091を設けた理由を以下に説明する。

図7に示すように、1394規格の1サイクルのうちに、1パケットのみを送信する場合には、暗号モードがたとえばモードA／偶数とモード／奇数と切り換わっても、各送信パケットには1394ヘッダのsy領域に暗号化情報が付加されることから、受信側で暗号モードを判別でき、復号可能である。

【0056】

これに対して、複数のパケットを暗号化して送信する場合には、暗号モード連續性判定回路1091を設けない場合には、図8に示すように、その切り替えタイミングにより1394規格の1サイクルのうちに、異なる暗号キーで暗号化されたデータが混在してしまう。

この場合、混在したデータに一つの1394ヘッダが付加されるのみであることから、受信側で複数の暗号モードを判別できず、復号することができなくなる。

【0057】

そこで、暗号モード連續性判定回路1091を設けて、複数をパケットの送信時に、FIFO112から送信データを読み出した際に暗号モードの連續性を確認し、不連續性を確認したときは、その1394規格の送信サイクルで送信できる帯域に余裕があったとしても送信を停止させ、次のサイクルで異なる暗号キーで暗号化されてパケットを送信するように、リンクコア101の送信回路に指示して、図9に示すように、1394規格の1サイクル内では、一つの暗号モード

で暗号化されたデータのみを送信し、異なる暗号モードで暗号化されたデータは次のサイクルで送信するように構成している。

【0058】

受信前処理回路110は、リンクコア101を介してIEEE1394シリアルバスB/Sを伝送されてきたアイソクロナス通信用パケットを受けて、受信パケットの1394ヘッダ、CIPヘッダ1, 2等の内容を解析し、4バイト(+4ビット)のソースパケットヘッダ(SPH)を付加し、受信用FIFO113に格納する。

【0059】

受信前処理回路110は、受信用FIFO113に受信データを格納するに際して、受信パケットの1394ヘッダのsy領域のビット3, 2, 1に設定されている暗号化情報を、送信前処理108と同様に格納するソースパケットヘッダおよびデータに付加する。

すなわち、図4(A)に示すように、4バイト(0~31ビット)のソースパケットヘッダに4ビット(32~36ビット)を付加し、この付加ビットのうちの33ビット、34ビット、および35ビットの3ビットを用いて暗号化情報を設定して格納するとともに、図4(B)に示すように、データ領域の4バイト(0~31ビット)の最大長を示すデータペイロード(Data Payload)に同じく4ビット(32~36ビット)を付加し、この付加ビットのうちの33ビット、34ビット、および35ビットの3ビットを用いて暗号化情報を設定して格納する。

【0060】

暗号化情報は、モードがビット[35:34]の2ビットで示され、キーの種類をビット[33]の1ビットで示され、内容に応じてこれら3ビットが、図2中sy[3:2]およびsy[1]のように設定される。ただし、ビット32は未使用である。

すなわち、モードAで偶数キーの場合には[111]、モードBで偶数キーの場合には[101]、モードCで偶数キーの場合には[011]、モードAで奇数キーの場合には[110]、モードBで奇数キーの場合には[100]、モードCで奇数キーの場合には[010]に設定される。

また、暗号化なしの場合には、ビット [35:34] が [00] に設定される。このとき、ビット [33] は意味を持たない。

【0061】

受信後処理回路111は、受信用FIFO113に格納されたソースパケットヘッダおよびデータを読み出して、付加された暗号化情報を暗号処理回路107の暗号モード検出回路1072に出力し、暗号化データをマルチプレクサ173を介して暗号エンジン回路1074に入力させる。

また、受信後処理回路111は、データ読み出し時においては、FIFO113に格納されたソースパケットヘッダのタイムスタンプの時間データを読み出し、読み出したタイムスタンプデータ (TS) とリンクコア101内にあるサイクルタイムによるサイクルタイム (CT) を比較し、サイクルタイムCTがタイムスタンプデータTSより大きい場合に、暗号エンジン回路1074で復号化されたデータをアプリケーションインターフェース回路103を介し、たとえばMPEG用トランスポートストリームデータとしてMPEGトランスポータ41へ出力させる。

【0062】

次に、IEEE1394シリアルインターフェースバスBSを伝送されるアイソクロナス通信用パケットの送信動作および受信動作を説明する。

【0063】

まず、CPU30からCFR114に、アイソクロナスパケットを暗号化する複数のモード (キー; key) が設定される。

そして、IEEE1394シリアルインターフェースバスBSにアイソクロナス通信用パケットを送出する場合には、設定された暗号モードのうちの一つを選択して暗号処理回路107が暗号化すべき暗号キー選択情報が、CPU30からホストインターフェース102を通してCFR114にセットされる。また、CPU30からは、アイソクロナス通信用パケットのSPH (ソースパケットヘッダ) に設定されるタイムスタンプ用遅延時間Txdelay がホストインターフェース102を通してCFR114にセットされる。

【0064】

これと並行して、アプリケーション側回路40のたとえばMPEGトランスポータ41によるMPEGトランSPORTストリームデータが、アプリケーションインターフェース回路103を介して暗号処理回路107に入力される。

【0065】

暗号処理回路107では、送信時にはアプリケーションインターフェース回路103を介した送信データが、マルチプレクサ1073を介して暗号エンジン回路1074に入力される。

また、暗号モード選択回路1071において、CPU30からCFR114に設定された暗号キー選択信号（情報）S114に基づき、CPU30からCFR114に設定された6個の暗号モード（キー；key）のうちの一の暗号キーが選択され、その情報が暗号エンジン回路1074に供給される。

【0066】

暗号エンジン回路1074においては、マルチプレクサ1073を介して入力した送信データが、暗号モード選択回路1071により指定された暗号キーに基づいて暗号化されて送信前処理回路108に出力される。

【0067】

送信前処理回路108では、暗号処理回路107による送信しへき暗号化データを受けて、IEEE1394規格のアイソクロナス通信用としてクワドレット（4バイト）単位にデータ長が調整され、かつ4バイト（+4ビット）のソースパケットヘッダ（SPH）を付加されて送信用 FIFO112に格納される。

このとき、送信前処理回路108では、送信用 FIFO112に送信データを格納するに際して、4バイト（0～31ビット）のソースパケットヘッダに4ビット（32～36ビット）が付加され、この付加ビットのうちの33ビット、34ビット、および35ビットの3ビットを用いて暗号化情報が設定され、併せて、データ領域の4バイト（0～31ビット）の最大長を示すデータペイロード(Data Payload)に同じく4ビット（32～36ビット）が付加され、この付加ビットのうちの33ビット、34ビット、および35ビットの3ビットを用いて暗号化情報が設定されて格納される。

【0068】

FIFO112に格納された送信データは、送信後処理回路109により読み出され、ソースパケットヘッダを含むデータに対して1394ヘッダ、CIPヘッダ1、2が付加されてリンクコア101の送信回路に出力される。

このとき、付加ビットに設定されていた暗号化情報s yは、1394ヘッダのビット[3, 2, 1]の3ビットに割り当てられてる。なお、その内容は、FIFO112に格納されたソースパケットヘッダに付加された暗号化情報に基づいて設定される。

【0069】

そして、リンクコア101の送信回路に入力されたパケットデータは、フィジカル・レイヤ回路20を介してIEEE1394シリアルインターフェースバスBSにアイソクロナス通信用パケットとして送出される。

【0070】

また、複数のパケットが暗号化されて送信される場合には、送信後処理回路109における暗号モード連続性判定回路1091において、FIFO112から送信データを読み出した際に暗号モードの連続性が確認される。

そして、不連続性が確認されたときは、その1394規格の送信サイクルで送信できる帯域に余裕があったとしても送信が停止され、次のサイクルで異なる暗号キーで暗号化されたパケットを送信するように、リンクコア101の送信回路に指示される。

これにより、1394規格の1サイクル内では、一つの暗号モードで暗号化されたデータのみが送信され、異なる暗号モードで暗号化されたデータは次のサイクルで送信される。

したがって、受信側で的確に暗号が解読され、データが復号される。

【0071】

IEEE1394シリアルバスBSを伝送されてきた、1394ヘッダに暗号化情報が設定されてるアイソクロナス通信用パケットは、フィジカル・レイヤ回路10、リンクコア101を介して受信前処理回路110に入力される。

【0072】

受信前処理回路110では、受信パケットの1394ヘッダ、CIPヘッダ1, 2等の内容が解析され、ソースパケットヘッダとデータがFIFO113に書き込まれる。

このとき、受信前処理回路110においては、受信用FIFO113に受信データを格納するに際して、4バイト(0~31ビット)のソースパケットヘッダに4ビット(32~36ビット)が付加され、この付加ビットのうちの33ビット、34ビット、および35ビットの3ビットを用いて暗号化情報が設定され、併せて、データ領域の4バイト(0~31ビット)の最大長を示すデータペイロード(Data Payload)に同じく4ビット(32~36ビット)が付加され、この付加ビットのうちの33ビット、34ビット、および35ビットの3ビットを用いて暗号化情報が設定されて格納される。

【0073】

そして、FIFO113に格納されたソースパケットヘッダおよび受信データは、受信後処理回路111により読み出され、付加ビットの暗号化情報が暗号処理回路107の暗号モード検出回路1072に供給され、暗号化データをマルチプレクサ173を介して暗号エンジン回路1074に供給される。

また、受信後処理回路111では、FIFO113に格納されたソースパケットヘッダのタイムスタンプの時間データが読み出され、読み出したタイムスタンプデータ(TS)とリンクコア101内にあるサイクルタイマによるサイクルタイム(CT)を比較し、サイクルタイムCTがタイムスタンプデータTSより大きい場合に、データ出力指示が暗号処理回路107の暗号エンジン回路1074に供給される。

【0074】

暗号処理回路107では、暗号モード検出回路1072において、受信後処理回路111を介して入力した暗号化されたデータに付加されている暗号化情報から、データの暗号化に用いられた暗号モード(キー)が検出される。そして、その検出結果が暗号キー選択信号S1072として暗号モード選択回路1071に出力される。

暗号モード選択回路1071においては、暗号キー選択信号S1072に基づき、CPU30からCFR114に設定された6個の暗号モード（キー；key）のうちの一の暗号キーが選択され、その情報が暗号エンジン回路1074に供給される。

【0075】

暗号エンジン回路1074は、マルチプレクサ1073を介して入力した受信データが、暗号モード選択回路1071により指定された暗号キーに基づいて復号される。

そして、復号されたデータが受信後処理回路111による指示時間に、アプリケーションインターフェース回路103を介し、たとえばMPEG用トランスポートストリームデータとしてMPEGトランスポータ41へ出力される。

【0076】

以上説明したように、本実施形態によれば、データ送信時には、CPU30からCFR114に設定された暗号キー選択信号S114に基づき、CPU30からCFR114に設定された6個の暗号モードのうちの一の暗号キーを選択し、データ受信時には、暗号モード検出回路1072からの暗号キー選択信号S1072に基づき、CPU30からCFR114に設定された6個の暗号モードのうち、一の暗号キーを選択する暗号モード選択回路1071と、受信パケットに附加されていた暗号化情報から、データの暗号化に用いられた暗号モードを検出し、検出結果を暗号キー選択信号S1072として暗号モード選択回路1071に出力する暗号モード検出回路1072と、送信時には、マルチプレクサ1073を介して入力した送信データを、暗号モード選択回路1071により指定された暗号キーに基づいて暗号化し、受信時には、マルチプレクサ1073を介して入力した受信データを、暗号モード選択回路1071により指定された暗号キーに基づいて暗号化データを復号する暗号エンジン回路1074とを有する暗号処理回路107と、送信時に、1394ヘッダに暗号化情報を設定して所定の送信パケットとして出力する送信後処理回路109とを設けたので、異なる機器間で送信または受信するデジタルデータの不正なコピーを防止でき、しかも良好なアイソクロナス通信を実現できる利点がある。

【0077】

また、本実施形態では、暗号モード連続性判定回路1091を設けて、複数をパケットの送信時に、FIFO112から送信データを読み出した際に暗号モードの連続性を確認し、不連続性を確認したときは、その1394規格の送信サイクルで送信できる帯域に余裕があったとしても送信を停止させ、次のサイクルで異なる暗号キーで暗号化されたパケットを送信するように、リンクコア101の送信回路に指示して、1394規格の1サイクル内では、一つの暗号モードで暗号化されたデータのみを送信し、異なる暗号モードで暗号化されたデータは次のサイクルで送信するように構成したので、受信側で複数の暗号モードを判別できず、復号できなくなるということを防止でき、受信側において暗号モードに応じて正しく復号することができる。

【0078】

なお、本実施形態では、アプリケーション側データとしてMPEGトランSPORTストリームデータを例に説明したが、本発明はこれに限定されず、デジタルオーディオ等、各デジタルデータに適用できることはいうまでもない。

【0079】

【発明の効果】

以上説明したように、本発明によれば、異なる機器間で送信または受信するデジタルデータの不正なコピーを防止できることはもとより、複数の暗号モードを判別できず、復号できなくなることを防止でき、受信側において受信データを正しく復号することができる信号処理回路を実現できる利点がある。

【図面の簡単な説明】

【図1】

IIEEE1394シリアルインターフェースに適用される本発明に係るMPEG用信号処理回路の一実施形態を示すブロック構成図である。

【図2】

本発明に係る暗号モードおよび暗号キーの例について説明するための図である

【図3】

本発明に係る暗号処理回路の構成例を示すブロック図である。

【図4】

FIFOに暗号化データを格納する場合に付加する暗号化情報の一形態を示す図である。

【図5】

送信時に1394ヘッダに暗号化情報を設定する一例を説明するための図である。

【図6】

本発明に係る送信後処理回路に暗号モード連続性判定回路を設けた例を示す図である。

【図7】

1サイクルに1パケットを送信する場合の通信形態を示す図である。

【図8】

1サイクルに複数のデータを送信する場合であって、暗号モード連続性判定回路を設けていない場合の通信形態を示す図である。

【図9】

1サイクルに複数のデータを送信する場合であって、暗号モード連続性判定回路を設けた場合の通信形態を示す図である。

【図10】

アイソクロナス通信における1ソースパケットのバイトサイズを示す図であって、(A)はDVB仕様時、(B)はDSS仕様時のパケットサイズを示す図である。

【図11】

IEEE1394規格のアイソクロナス通信でデータを送信させるとときの元のデータと、実際に送信されるパケットとの対応関係の一例を示す図である。

【図12】

ソースパケットヘッダのフォーマットを示す図である。

【図13】

アイソクロナス通信用パケットの基本構成例を示す図である。

【図14】

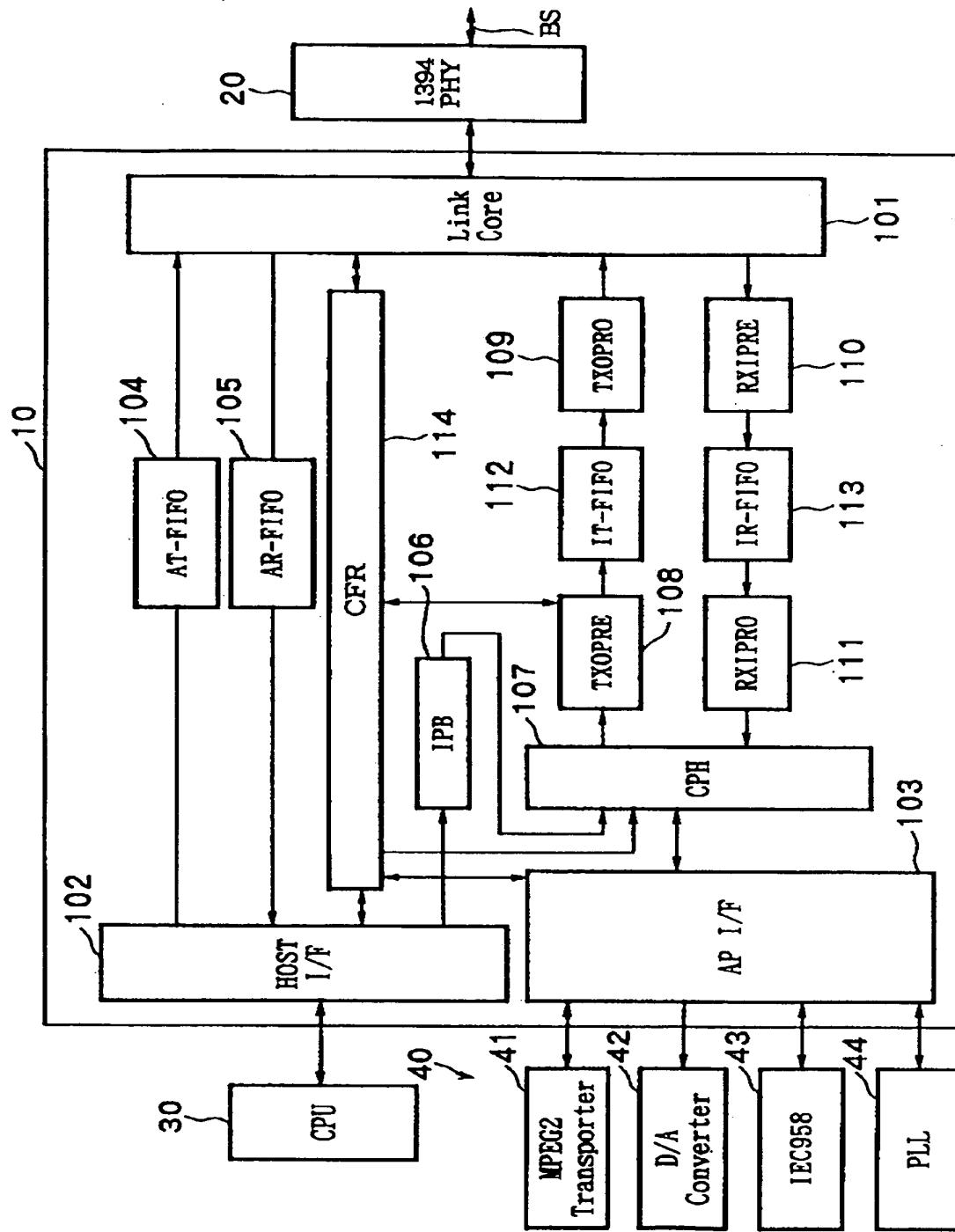
I E E E 1 3 9 4 シリアルインターフェースにおけるアイソクロナス通信系回路の基本構成を示すブロック図である。

【符号の説明】

1 0 … リンク・レイヤ回路、 1 0 1 … リンクコア (Link Core) 、 1 0 2 … ホストインターフェース回路 (Host I/F) 、 1 0 3 … アプリケーションインターフェース回路 (AP I/F) 、 1 0 4 … アシンクロナス通信の送信用 FIFO (AT-FIFO) 、 1 0 5 … アシンクロナス通信の受信用 FIFO (AR-FIFO) 、 1 0 6 … インサートパケットバッファ (IPB) 、 1 0 7 … 暗号処理回路、 1 0 7 1 … 暗号モード選択回路、 1 0 7 2 … 暗号モード検出回路、 1 0 7 3 … マルチプレクサ、 1 0 7 4 … 暗号エンジン回路、 1 0 8 … アイソクロナス通信用送信前処理回路 (TXOPRE) 、 1 0 9 … アイソクロナス通信用送信後処理回路 (TXOPRO) 、 1 0 9 1 … 暗号モード連続性判定回路、 1 1 0 … アイソクロナス通信用受信前処理回路 (TXPRE) 、 1 1 1 … アイソクロナス通信用受信後処理回路 (TXIPRO) 、 1 1 2 … アイソクロナス通信の送信用 FIFO (IT-FIFO) 、 1 1 3 … アイソクロナス通信の受信用 FIFO (IR-FIFO) 、 1 1 4 … コンフィギュレーションレジスタ (CFR) 、 2 0 … フィジカル・レイヤ回路、 3 0 … CPU 、 4 0 … アプリケーション側回路、 4 1 … MPEG トランスポータ、 4 2 … D/A コンバータ、 4 3 … IEC 958 ディジタルオーディオ回路、 4 4 … PLL 回路。

【書類名】 図面

【図1】



【図2】

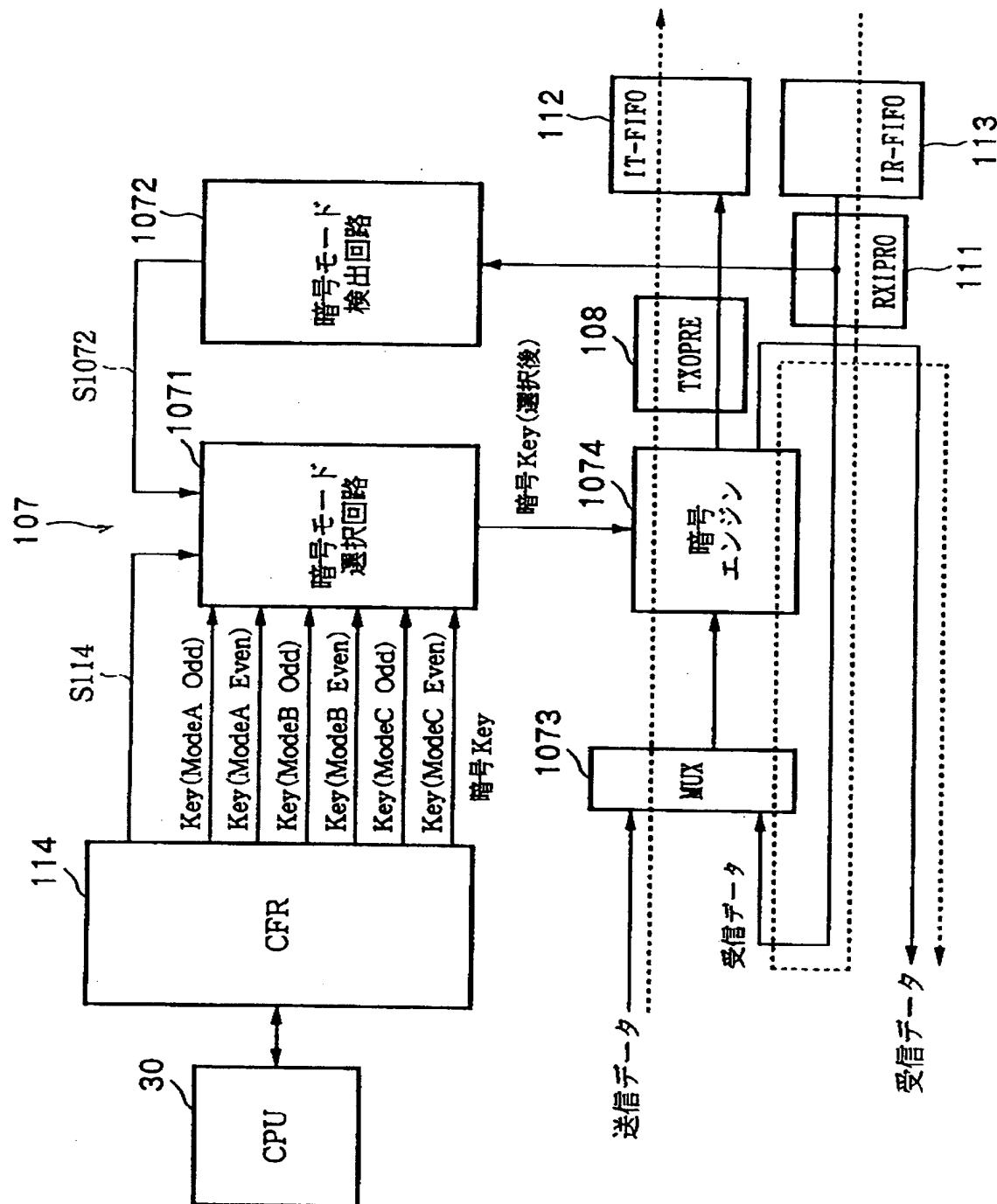
sy[3:2]	暗号モード	内 容
11	モードA	Never Copy
10	モードB	Copy Once
01	モードC	No More Copy
00	暗号化なし	Copy Free

(A)

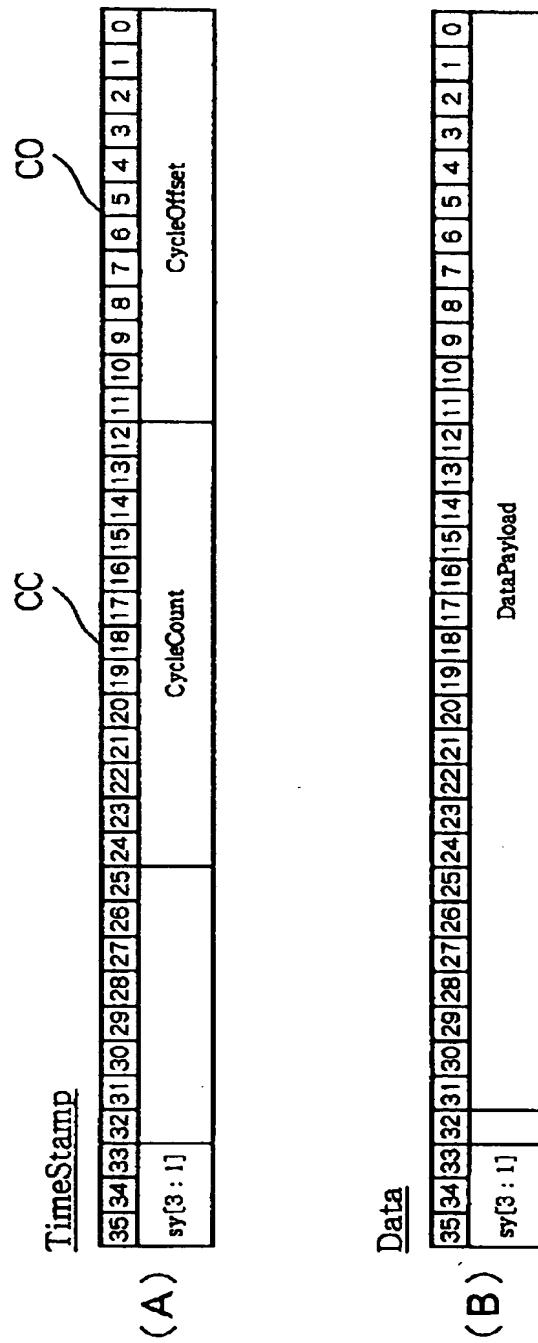
sy[1]	暗号Keyの種類
1	Even Key
0	Odd Key

(B)

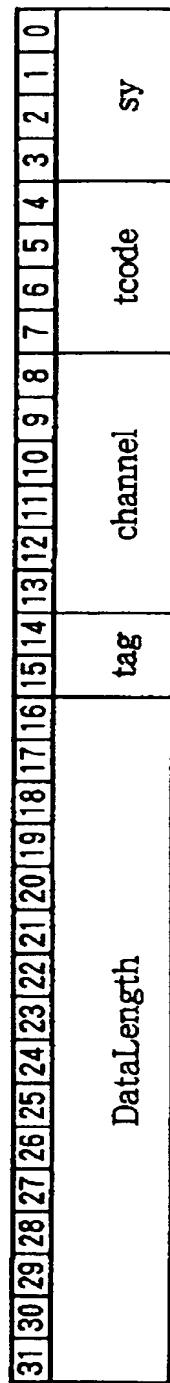
【図3】



【図4】

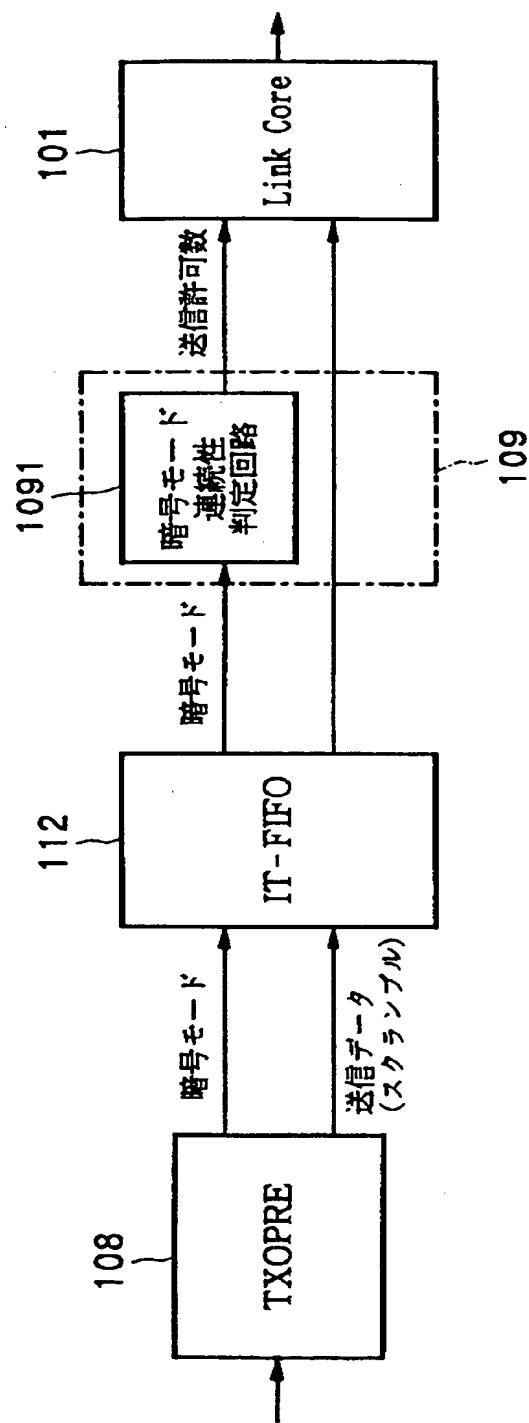


【図5】



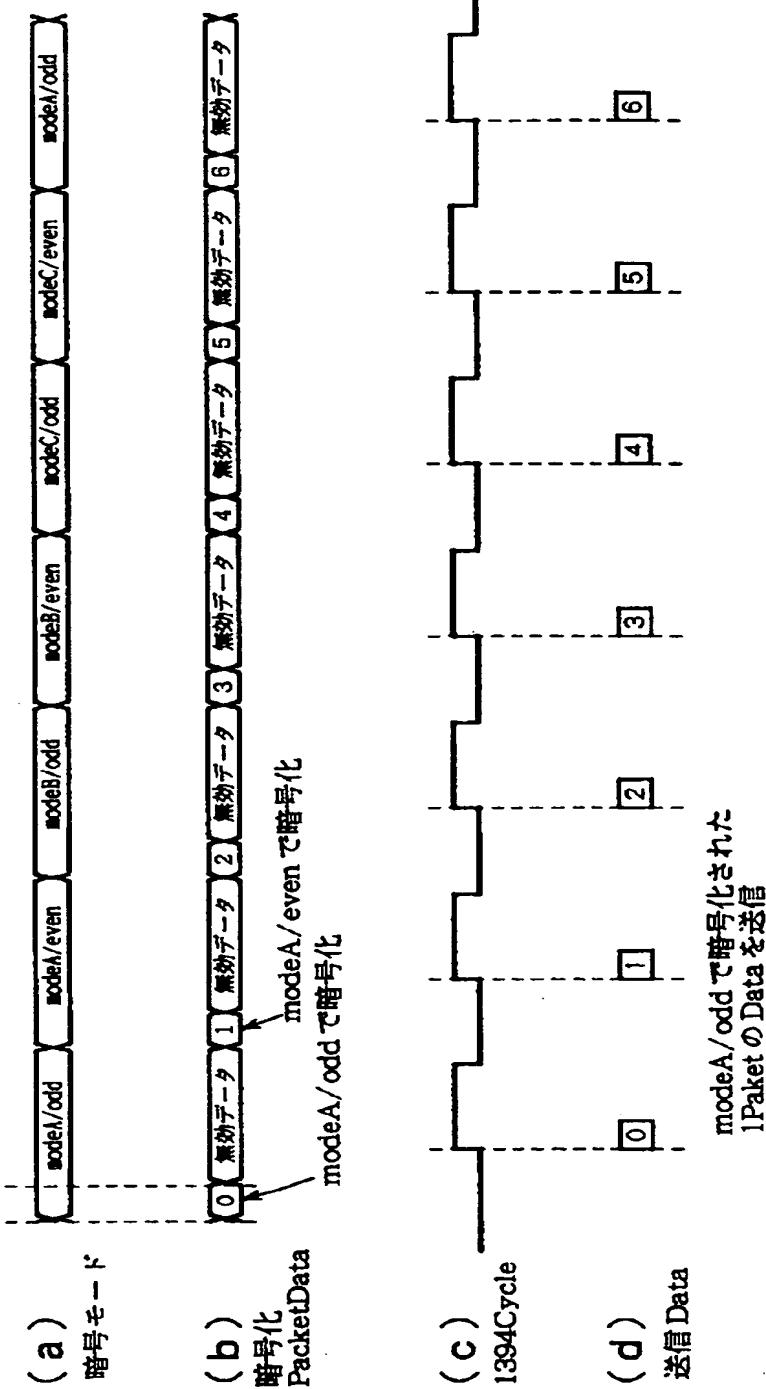
sy[3:0] の bit3-bit1 を暗号モードに割り当てる。

【図6】

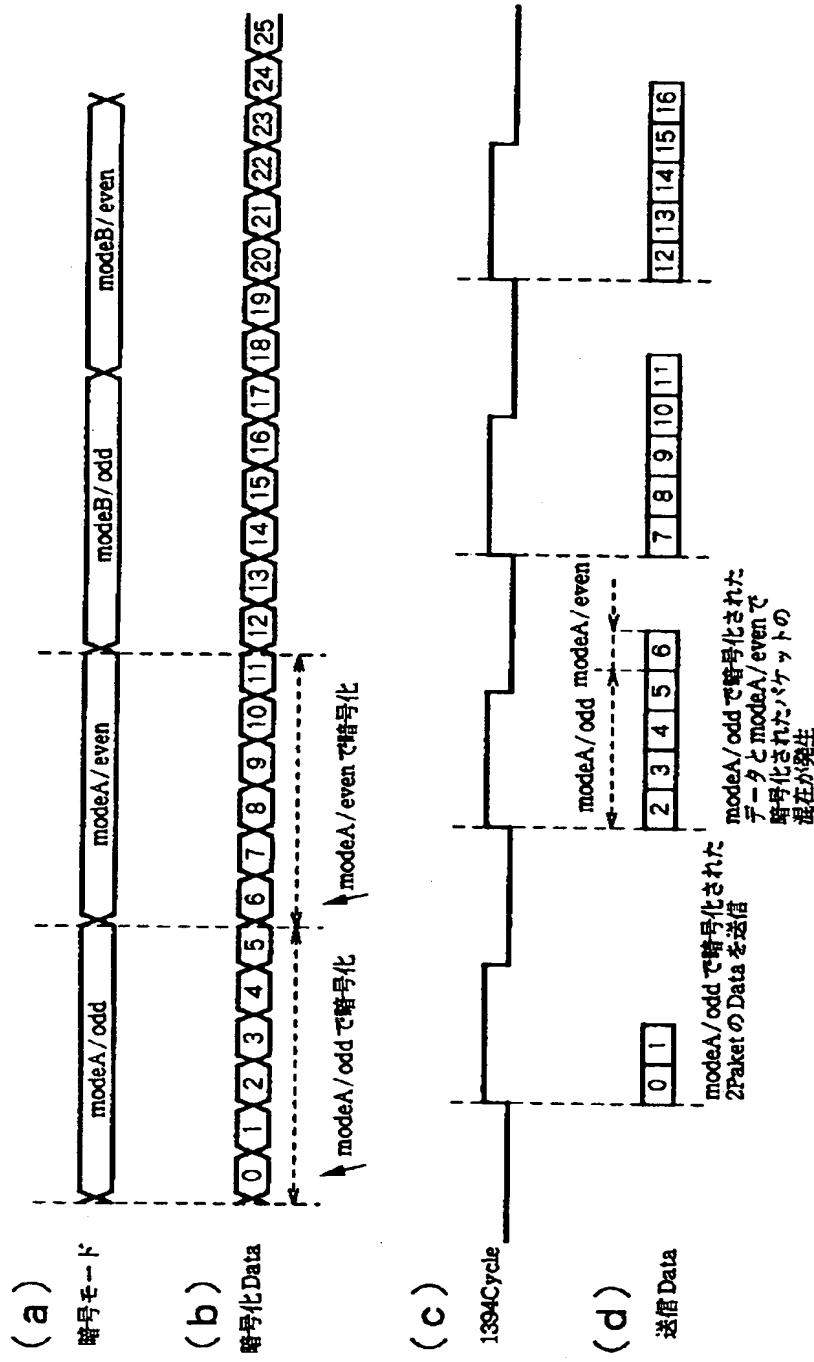


【図7】

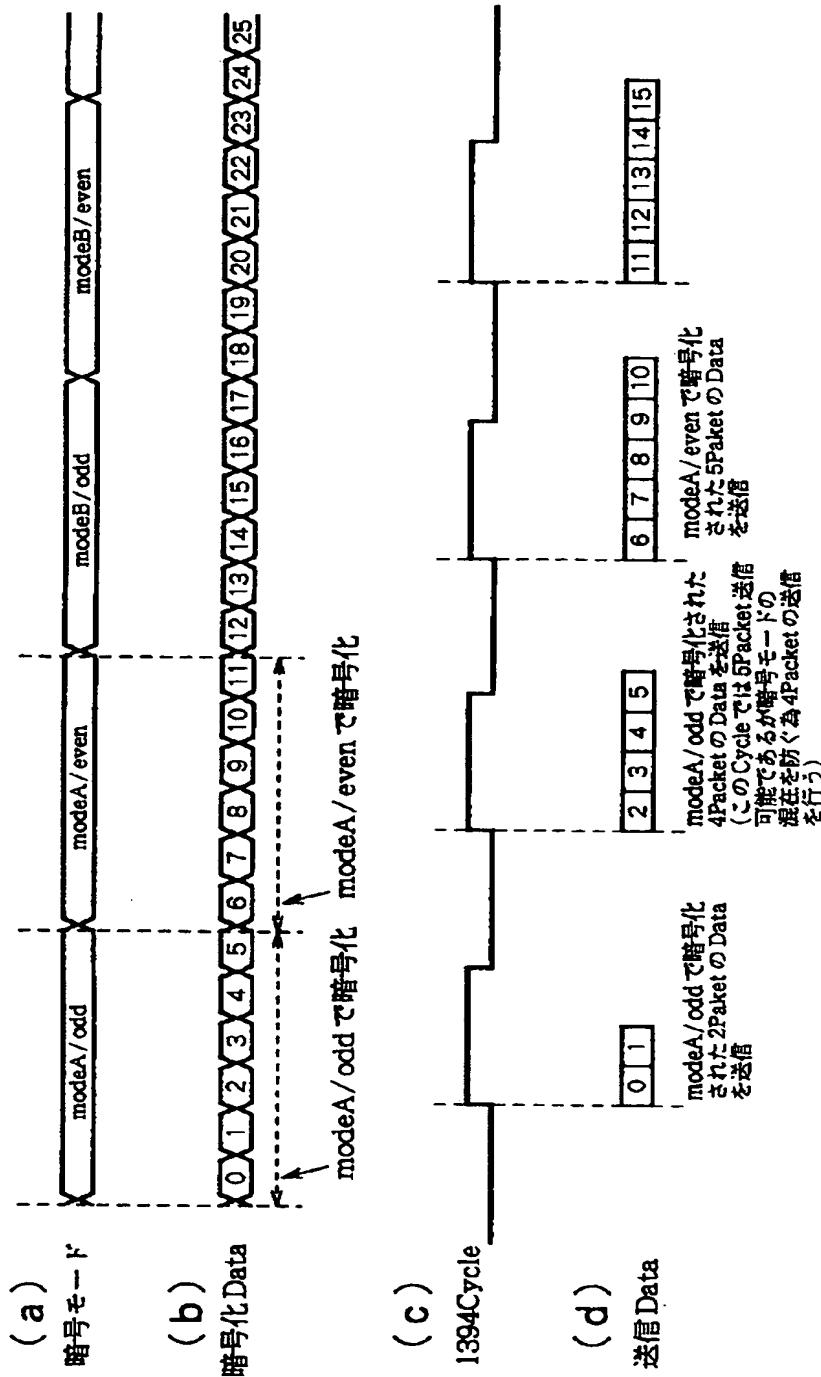
1Cycleに1Packetのデータを送信する場合



【図8】



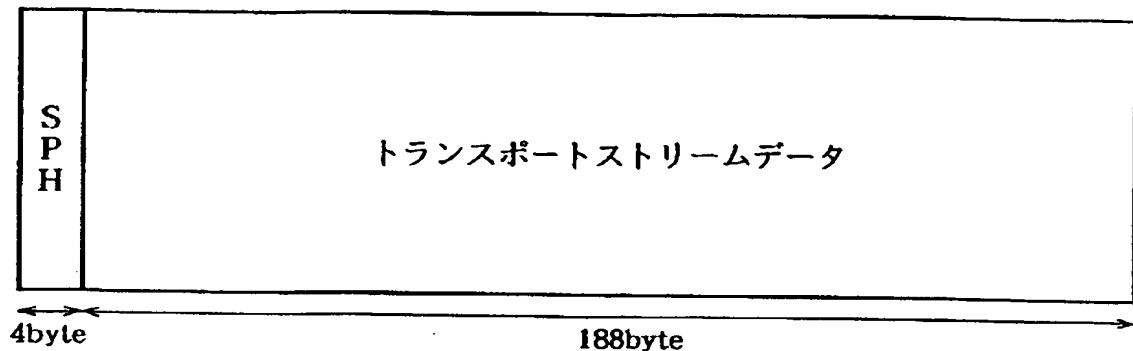
【図9】



【図10】

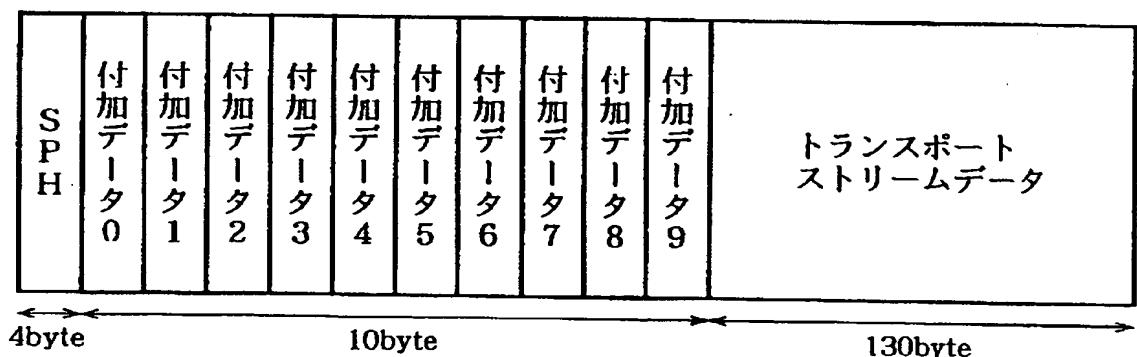
(A)

DVB

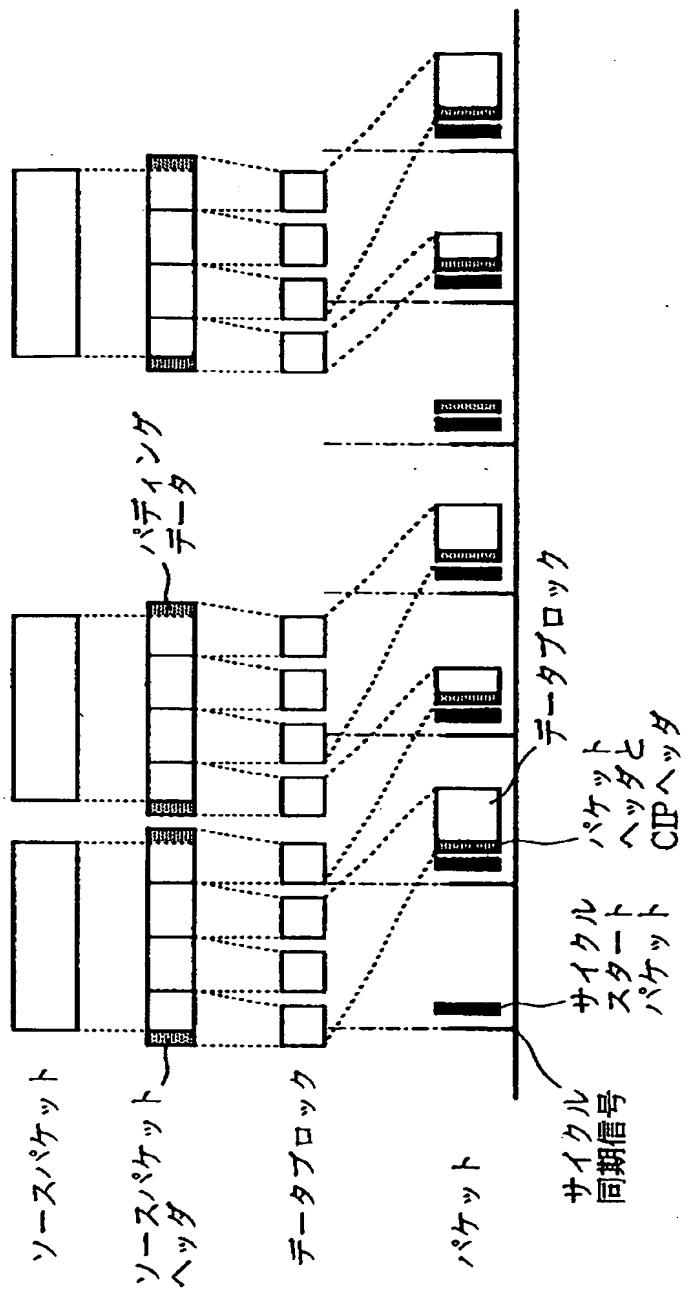


(B)

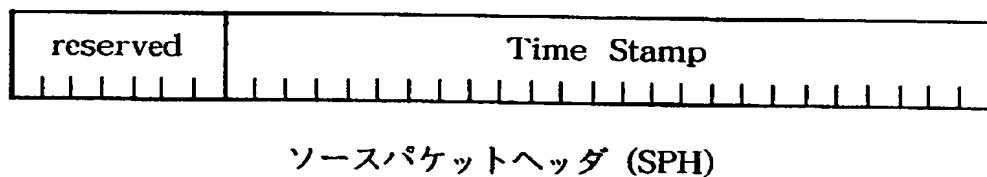
DSS



【図11】

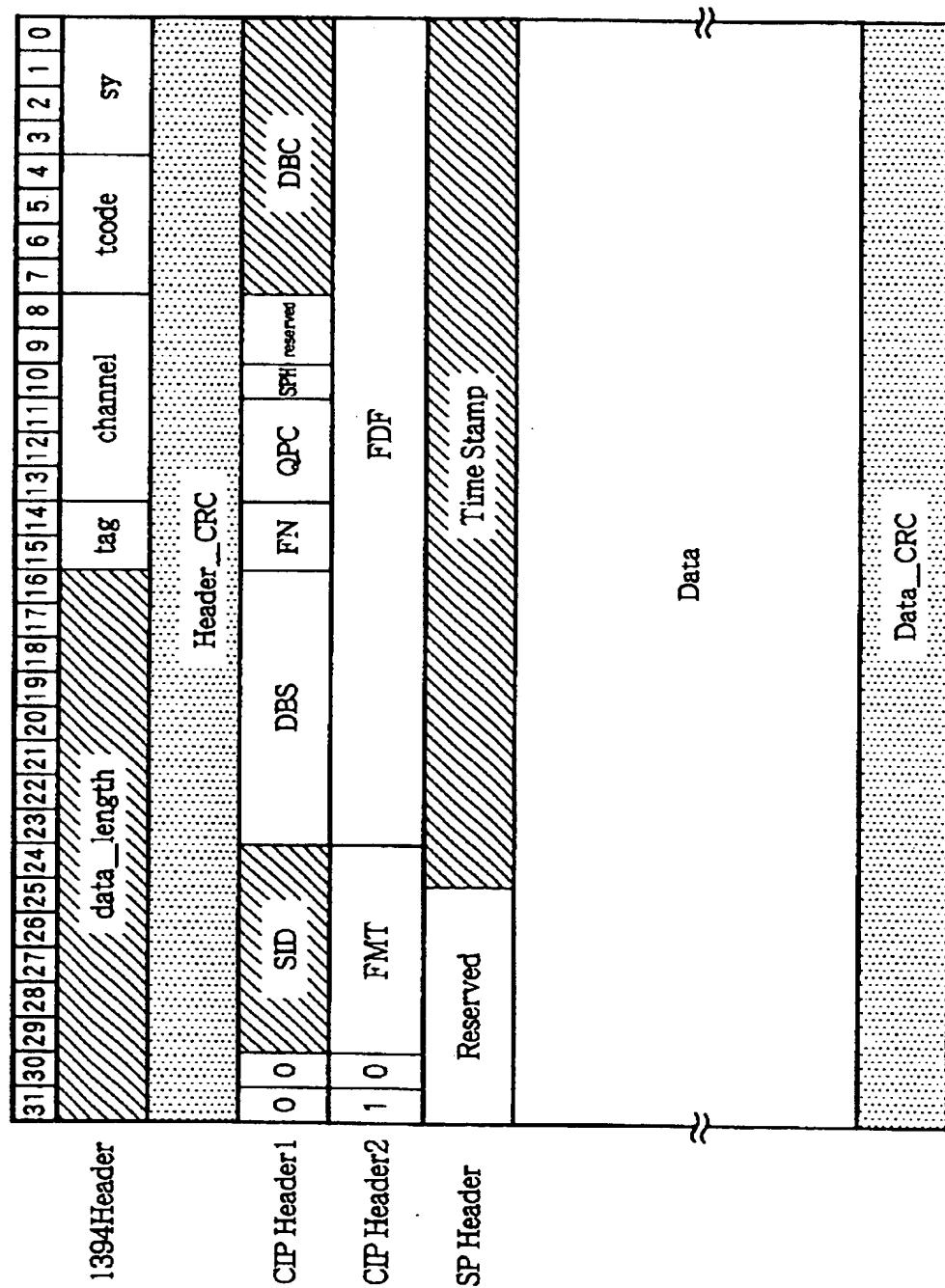


【図12】

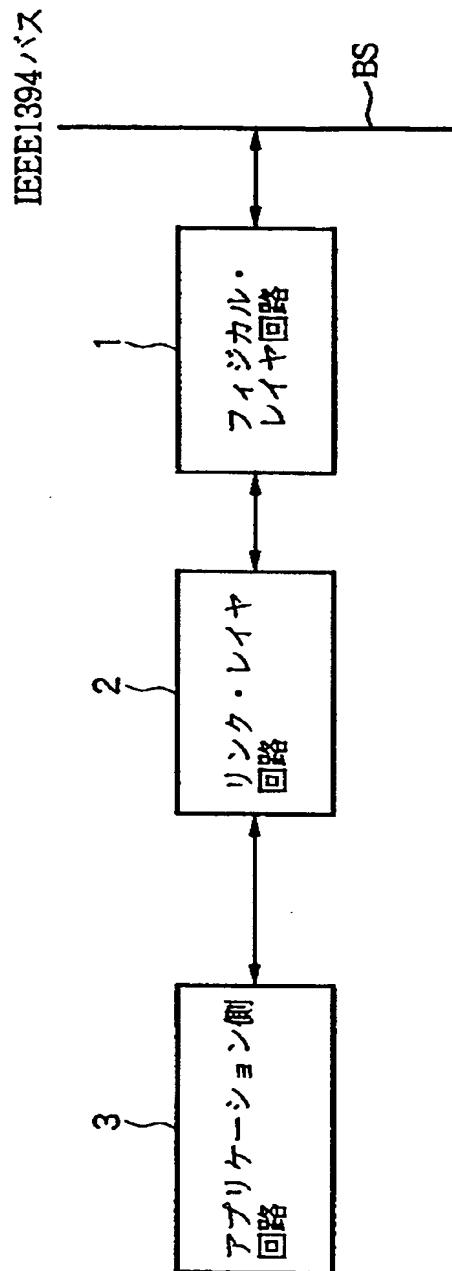


ソースパケットヘッダ (SPH)

【図13】



【図14】



【書類名】 要約書

【要約】

【課題】 不正なコピーを防止しつつ、かつ複数の暗号モードを判別できず、復号できなくなることを防止でき、受信側において受信データを正しく復号することができる信号処理回路を提供する。

【解決手段】 暗号モード連続性判定回路1091を設け、複数をパケットの送信時に、FIFO112から送信データを読み出した際に暗号モードの連続性を確認し、不連続性を確認したときは、その1394規格の送信サイクルで送信できる帯域に余裕があったとしても送信を停止させ、次のサイクルで異なる暗号キーで暗号化されたパケットを送信するように、リンクコア101の送信回路に指示して、1394規格の1サイクル内では、一つの暗号モードで暗号化されたデータのみを送信し、異なる暗号モードで暗号化されたデータは次のサイクルで送信するように構成する。

【選択図】 図6

【書類名】 職権訂正データ
【訂正書類】 特許願

＜認定情報・付加情報＞

【特許出願人】

【識別番号】 000002185

【住所又は居所】 東京都品川区北品川6丁目7番35号

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100094053

【住所又は居所】 東京都台東区柳橋2丁目4番2号 創進国際特許事務所

【氏名又は名称】 佐藤 隆久

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社